OIPE
JAN 2 8 2008
PATENT & TRADEMARK OFFICE

AF
TD

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

**PATENT APPLICATION**

ATTORNEY DOCKET NO. **10012790-1**

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Inventor(s):** Philip M. WALKER et al.

**Confirmation No.:** 9299

**Application No.:** 09/903,278

**Examiner:** Tran, Tongoc

**Filing Date:** July 11, 2001

**Group Art Unit:** 2134

**Title:** SYSTEM AND METHOD OF VERIFYING SYSTEM ATTRIBUTES

Mail Stop Appeal Brief - Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

## TRANSMITTAL OF REPLY BRIEF

Transmitted herewith is the Reply Brief with respect to the Examiner's Answer mailed on November 27, 2007 .

This Reply Brief is being filed pursuant to 37 CFR 1.193(b) within two months of the date of the Examiner's Answer.

(Note: Extensions of time are not allowed under 37 CFR 1.136(a))

(Note: Failure to file a Reply Brief will result in dismissal of the Appeal as to the claims made subject to an expressly stated new ground rejection.)

No fee is required for filing of this Reply Brief.

If any fees are required please charge Deposit Account 08-2025.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit: January 25, 2008

**OR**

□ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300.
Date of facsimile:

Typed Name: Cindy C. Dioso
Signature: Cindy C. Dioso

Respectfully submitted,
Philip M. WALKER et al.

By James L Baudino
James L. Baudino
Attorney/Agent for Applicant(s)

Reg No. : 43,486
Date : January 25, 2008
Telephone : 214-855-7544

OIPE IAP14
JAN 2 8 2008
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

## APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | | | |
|---|---|---|---|
| In re Application of: | Philip M. WALKER et al. | Confirmation No.: | 9299 |
| Serial No.: | 09/903,278 | | |
| Filing Date: | July 11, 2001 | | |
| Group Art Unit: | 2134 | | |
| Examiner: | Tran, Tongoc | | |
| Title: | SYSTEM AND METHOD OF VERIFYING SYSTEM ATTRIBUTES | | |
| Docket No.: | 10012790-1 | | |

**MAIL STOP: APPEAL BRIEF-PATENTS**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

## REPLY BRIEF

Appellant respectfully submits this Reply Brief in response to the Examiner's Answer mailed November 27, 2007, pursuant to 37 C.F.R. § 1.193(b).

## STATUS OF CLAIMS

Claims 1-26 stand rejected pursuant to a final Office Action mailed March 1, 2007 (hereinafter, the "Office Action"). Claims 1-26 are presented for appeal.

## GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-17, 19-24 and 26 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,978,475 issued to Schneier et al. (hereinafter "*Schneier*").

2. Claims 1, 10 and 19 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,088,804 issued to Hill et al. (hereinafter "*Hill*").

3. Claims 18 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Schneier*.

## ARGUMENT

1. Rejection under 35 U.S.C. § 102(b) in view of *Schneier*

a. Claims 1-5, 7, 9-14, 17, 19-24 and 26

Claim 1, for example, recites "a probe operable to execute in the target and collect a predetermined set of data associated with the target" and "a monitor operable to receive the collected predetermined set of data to **compare with expected data values**" (emphasis added). In the Examiner's Answer, the Examiner appears to confuse: 1) the attributes of a client or target system that may be compared with **expected values** to determine whether the target system has been altered; with 2) data produced by the target system and whether the data is reliable. In the Examiner's Answer, the Examiner considers any information received from the target system as meeting the limitations of Claim 1 (Examiner's Answer, pages 9 and 10). Appellant respectfully disagrees.

In the Examiner's Answer, the Examiner refers to various portions of Appellant's specification to apparently illustrate that the "probe" recited by Claim 1 can obtain different types of data from a target system (Examiner's Answer, pages 9 and 10). The Examiner then appears to improperly label the different types of information as "attributes" so that the Examiner can consider *Schneier*'s audit log as an "attribute" in order to support the Examiner's rationale for rejecting Claim 1 (Examiner's Answer, page 10). Appellant respectfully submits that the Examiner's rationale results in an improper rejection of Claim 1. Appellant respectfully refers the Board to the following portions of Appellant's specification:

> [P]robe 20 gets attribute data associated with the client systems such as verification data **and** billing data.

(page 3, lines 30-31) (emphasis added).

> **Verification data** comprises any information acquired or inferred by the process of sampling and/or modifying various aspects of the target system, involving physical hardware state and/or system files. Probe 20 has instructions to gather data on a list of system attributes and parameters from client system 16. System attributes and parameters may include a serial number of the CPU (central processing unit) or another system component, the current disk type, the dates, size, or other parameters of a specific set of system files, the physical position on a disk drive of certain system files, the network MAC (media access control) address, etc.

(page 3, line 31 to page 4, line 7) (emphasis added).

> Furthermore, probe 20 is optionally instructed to obtain information on usage, such as memory usage, disk storage usage, CPU usage, etc. **for billing purposes**.

(page 4, lines 7-9) (emphasis added).

> Monitor 14 **checks the verification data** returned by probe 20 **to determine whether they matched the expected values**. **If there is a mismatch**, there is a possibility that client system 16 has been altered in an unauthorized manner and that **the returned usage data may not be trustworthy**.

(page 4, lines 14-17) (emphasis added).

In the Examiner's Answer, the Examiner appears to consider the "predetermined set of data" and the "expected data values" recited by Claim 1 as relative data sets, and the Examiner appears to consider either the verification data or the billing data to meet these limitations (Examiner's Answer, page 10). However, as indicated above, it is the **verification data that is compared to expected values**.

Further, the Examiner appears to assert that because the audit log of *Schneier* is a "file," the audit log of *Schneier* thereby qualifies as "verification data" (Examiner's Answer, pages 10 and 11). Appellant respectfully disagrees. As indicated in Appellant's Appeal Brief, *Schneier* appears to disclose that the audit log 300 of *Schneier* is a collection of entries indicating, for example, a type of action that is being logged, the person or computer that initiated the action, the results or effects of the action, successful and unsuccessful log-ins, log-offs, remote log-ins, etc. (*Schneier*, column 6, lines 42-64). Thus, the audit log 300 of *Schneier* appears to be data representative of entirely unexpected or random occurrences associated with a computer in *Schneier*. Thus, Appellant respectfully submits that the audit log 300 of *Schneier* is not "**compare[d] with expected values**" as recited by Claim 1 (emphasis added) to determine whether the target computer in *Schneier* has been altered at least because the information of the audit log 300 of *Schneier* appears to be completely unexpected and/or random based on what acts or events happen to take place or occur with the computer of *Schneier*. Accordingly, for at least these reasons, Claim 1 is patentable over *Schneier*.

Independent Claim 10 recites "executing a probe in a target" and "collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered" (emphasis added). Independent Claim 19 recites "initiating the execution of a probe in a target," "receiving from the probe a predetermined set of data associated with the target" and "comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered" (emphasis added). At least for the reasons discussed above in connection with independent Claim 1, Appellant respectfully submits that independent Claims 10 and 19 are also not anticipated by *Schneier.*

Claims 2-5, 7, 9, 11-14, 17, 18-24 and 26 depend respectively from independent Claims 1, 10 and 19. Therefore, for at least this reason, Appellant respectfully submits that Claims 2-5, 7, 9, 11-14, 17, 18-24 an 26 are also allowable over *Schneier.*

Accordingly, for at least the reasons discussed above, independent Claims 1, 10 and 19 are clearly patentable over *Schneier.* Therefore, Claims 1, 10 and 19, and Claims 2-5, 7, 9, 11-14, 17, 18-24 and 26 that depend respectively therefrom, are in condition for allowance.

b. Claim 6

Appellant respectfully repeats and maintains the arguments presented in Appellant's Appeal Brief regarding Claim 6, and Appellant respectfully submits that Claim 6 is patentable over the cited reference. Further, in the Examiner's Answer, the Examiner appears to assert that because *Schneier* discloses a cryptographic module 165/220, *Schneier* necessarily anticipates Claim 6 (Examiner's Answer, pages 11 and 12). For example, in the Examiner's Answer, the Examiner appears to refer to a "hash" function purportedly performed by the cryptographic module 220 of *Schneier,* and the Examiner appears to indicate that because *Schneier* purportedly teaches "tools for implementing various cryptographic techniques," *Schneier* anticipates Claim 6 (Examiner's Answer, pages 11 and 12). Appellant respectfully disagrees. Appellant respectfully submits that *Schneier* does not appear to disclose or even suggest that the audit logging program 200 of *Schneier* (which the Examiner appears to consider as corresponding to the "probe" recited by Claim 1) calculates a signature value of at least a portion of an execution image of the audit logging program 200 of *Schneier,* nor has the Examiner explicitly identified any such disclosure in *Schneier.* Accordingly, Claim 6 is patentable over *Schneier.*

c. Claim 8

Appellant respectfully repeats and maintains the arguments presented in Appellant's Appeal Brief regarding Claim 8, and Appellant respectfully submits that Claim 8 is patentable over the cited reference. Further, in the Examiner's Answer, the Examiner appears to assert that because *Schneier* discloses a cryptographic module 165/220, *Schneier* necessarily anticipates Claim 8 (Examiner's Answer, pages 11-13). For example, in the Examiner's Answer, the Examiner appears to refer to a "hash" function purportedly performed by the cryptographic module 220 of *Schneier*, and the Examiner appears to indicate that because *Schneier* purportedly teaches "tools for implementing various cryptographic techniques," *Schneier* anticipates Claim 8 (Examiner's Answer, pages 11-13). Appellant respectfully disagrees. Appellant respectfully submits that *Schneier* does not appear to disclose or even suggest that the audit logging program 200 of *Schneier* (which the Examiner appears to consider as corresponding to the "probe" recited by Claim 1) determines a signature value of a random subset of an execution image of the audit logging program 200 of *Schneier*, nor has the Examiner explicitly identified any such disclosure in *Schneier*. Accordingly, Claim 8 is patentable over *Schneier*.

d. Claim 15

Appellant respectfully repeats and maintains the arguments presented in Appellant's Appeal Brief regarding Claim 15, and Appellant respectfully submits that Claim 15 is patentable over the cited reference. Further, in the Examiner's Answer, the Examiner appears to assert that because *Schneier* discloses a cryptographic module 165/220, *Schneier* necessarily anticipates Claim 15 (Examiner's Answer, pages 11-13). For example, in the Examiner's Answer, the Examiner appears to refer to a "hash" function purportedly performed by the cryptographic module 220 of *Schneier*, and the Examiner appears to indicate that because *Schneier* purportedly teaches "tools for implementing various cryptographic techniques," *Schneier* anticipates Claim 15 (Examiner's Answer, pages 11-13). Appellant respectfully disagrees. Appellant respectfully submits that *Schneier* does not appear to disclose or even suggest that the audit logging program 200 of *Schneier* (which the Examiner appears to consider as corresponding to the "probe" recited by Claim 10) calculates a signature value of at least a portion of the audit logging program 200 of *Schneier* for comparison to an expected signature value, nor has the Examiner explicitly identified any such disclosure in *Schneier*. Accordingly, Claim 15 is patentable over *Schneier*.

e. Claim 16

Appellant respectfully repeats and maintains the arguments presented in Appellant's Appeal Brief regarding Claim 16, and Appellant respectfully submits that Claim 16 is patentable over the cited reference. Further, in the Examiner's Answer, the Examiner appears to assert that because *Schneier* discloses a cryptographic module 165/220, *Schneier* necessarily anticipates Claim 16 (Examiner's Answer, pages 11-13). For example, in the Examiner's Answer, the Examiner appears to refer to a "hash" function purportedly performed by the cryptographic module 220 of *Schneier*, and the Examiner appears to indicate that because *Schneier* purportedly teaches "tools for implementing various cryptographic techniques," *Schneier* anticipates Claim 16 (Examiner's Answer, pages 11-13). Appellant respectfully disagrees. Appellant respectfully submits that *Schneier* does not appear to disclose or even suggest that the audit logging program 200 of *Schneier* (which the Examiner appears to consider as corresponding to the "probe" recited by Claim 10) calculates a signature value of the audit logging program 200 of *Schneier* for comparison to an expected signature value, nor has the Examiner explicitly identified any such disclosure in *Schneier*. Accordingly, Claim 16 is patentable over *Schneier*.

2. Rejection under 35 U.S.C. §102(b) in view of *Hill*

a. Claim 1

Independent Claim 1 recites "a probe operable to execute in the target and collect **a predetermined set of data** associated with the target" and "a monitor operable to receive the collected predetermined set of data to **compare with expected data values** **to determine whether the target has been altered**" (emphasis added).

In the Examiner's Answer, the Examiner relies on the SOM processor 40 of *Hill* to "receive the collected predetermined set of data to compare with expected data values" as recited by Claim 1 (Examiner's Answer, page 14). However, Claim 1 recites that the monitor "receive[s] the collected predetermined set of data to compare with **expected data values** **to determine whether the target has been altered**" (emphasis added). In *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). In the Examiner's Answer, the Examiner relies on a training process of *Hill* where the SOM processor 40 of *Hill* maps various training signatures to various display map regions so that when actual attack information is received, a network manager is provided with attack type and severity (*Hill*, column 6, line 61 to column 7, line 8). Thus, the SOM processor 40 of *Hill* does not appear to make any comparison "to determine whether the target has been altered" as recited by Claim 1. To the contrary, the SOM processor 40 is determining what action or response to take **to an identified attack**. Further, it is the map regions 70, 72 and 74 of *Hill* that define the type and severity of an attack, and not any comparison performed by the SOM processor of *Hill*.

For example, *Hill* appears to disclose that in response to a security event at a node of the network, an attack signature is sent to the SOM processor 40 by the security agent(s) 36 operating at the node(s) of *Hill* (*Hill*, column 7, line 64 to column 8, line 21). *Hill* further appears to disclose that that the SOM processor 40 compares a vector representation of an attack signature to the training signatures to select one that most closely matches so that a mitigation list of recommended actions that may be taken is generated (*Hill*, column 8, lines 35-58). Thus, it appears as though by the time the SOM processor 40 receives an attack signature from the security agent 36 of *Hill*, the security agent 36 of *Hill* has already determined that an attack has occurred. Thus, Appellant submits that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 1. To the contrary, a determination that the target (node) in *Hill* has been altered appears to be established before the SOM processor 40 performs any function. The SOM processor 40 appears to be used to determine what mitigating actions may be taken in response to an attack.

Further, Claim 1 recites that “the collected predetermined set of data [is] compare[d] with **expected data values**” (emphasis added). The “expected data values” correspond to data values expected for the target. Appellant respectfully submits that any purported comparison performed by the SOM processor 40 of *Hill* is not with “expected data values” corresponding to the target.

Appellant respectfully submits that for at least this reason, *Hill* does not anticipate Claim 1.

b. Claim 10

Independent Claim 10 recites “executing a probe in a target" and "collecting a predetermined set of data associated with the target for **comparison with expected**

**data values** for the predetermined set of data **to determine whether the target has been altered**" (emphasis added).

In the Examiner's Answer, the Examiner relies on the SOM processor 40 of *Hill* to "collect[] a predetermined set of data associated with the target for **comparison with expected data values**" as recited by Claim 10 (Examiner's Answer, page 14). However, Claim 10 recites "collecting a predetermined set of data associated with the target for **comparison with expected data values** for the predetermined set of data **to determine whether the target has been altered**" (emphasis added). In *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). In the Examiner's Answer, the Examiner relies on a training process of *Hill* where the SOM processor 40 of *Hill* maps various training signatures to various display map regions so that when actual attack information is received, a network manager is provided with attack type and severity (*Hill*, column 6, line 61 to column 7, line 8). Thus, the SOM processor 40 of *Hill* does not appear to make any comparison "to determine whether the target has been altered" as recited by Claim 10. To the contrary, the SOM processor 40 is determining what action or response to take **to an identified attack**. Further, it is the map regions 70, 72 and 74 of *Hill* that define the type and severity of an attack, and not any comparison performed by the SOM processor of *Hill*.

For example, *Hill* appears to disclose that in response to a security event at a node of the network, an attack signature is sent to the SOM processor 40 by the security agent(s) 36 operating at the node(s) of *Hill* (*Hill*, column 7, line 64 to column 8, line 21). *Hill* further appears to disclose that that the SOM processor 40 compares a vector representation of an attack signature to the training signatures to select one that most closely matches so that a mitigation list of recommended actions that may be taken is generated (*Hill*, column 8, lines 35-58). Thus, it appears as though by the time the SOM processor 40 receives an attack signature from the security agent 36 of *Hill*, the security agent 36 of *Hill* has already determined that an attack has occurred. Thus, Appellant submits that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 10. To the contrary, a determination that the target (node) in *Hill* has been altered appears to be established before the SOM processor 40 performs any function. The SOM processor 40 appears to be used to determine what mitigating actions may be taken in response to an attack.

Further, Claim 10 recites that the "predetermined set of data associated with the target" is compared "with **expected data values for the predetermined set of data**" (emphasis added). The "expected data values" correspond to data values expected for the target. Appellant respectfully submits that any purported comparison performed by the SOM processor 40 of *Hill* is not with "expected data values" corresponding to the target

Appellant respectfully submits that for at least this reason, *Hill* does not anticipate Claim 10.

c. Claim 19

Independent Claim 19 recites "initiating the execution of a probe in a target," "receiving from the probe a predetermined set of data associated with the target" and "**comparing** the received predetermined set of data **with expected data values** thereof **to determine whether the target has been altered**" (emphasis added).

In the Examiner's Answer, the Examiner relies on the SOM processor 40 of *Hill* to "**compar[e]** the received predetermined set of data **with expected data values**" as recited by Claim 19 (Examiner's Answer, page 14). However, Claim 19 recites "**comparing** the received predetermined set of data **with expected data values** thereof **to determine whether the target has been altered**" (emphasis added). In *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). In the Examiner's Answer, the Examiner relies on a training process of *Hill* where the SOM processor 40 of *Hill* maps various training signatures to various display map regions so that when actual attack information is received, a network manager is provided with attack type and severity (*Hill*, column 6, line 61 to column 7, line 8). Thus, the SOM processor 40 of *Hill* does not appear to make any comparison "to determine whether the target has been altered" as recited by Claim 19. To the contrary, the SOM processor 40 is determining what action or response to take **to an identified attack**.

Further, it is the map regions 70, 72 and 74 of *Hill* that define the type and severity of an attack, and not any comparison performed by the SOM processor of *Hill*.

For example, *Hill* appears to disclose that in response to a security event at a node of the network, an attack signature is sent to the SOM processor 40 by the security agent(s) 36 operating at the node(s) of *Hill* (*Hill*, column 7, line 64 to column 8, line 21). *Hill* further appears to disclose that that the SOM processor 40 compares a vector representation of an attack signature to the training signatures to select one that most closely matches so that a mitigation list of recommended actions that may be taken is generated (*Hill*, column 8, lines 35-58). Thus, it appears as though by the time the SOM processor 40 receives an attack signature from the security agent 36 of *Hill*, the security agent 36 of *Hill* has already determined that an attack has occurred. Thus, Appellant submits that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 19. To the contrary, a determination that the target (node) in *Hill* has been altered appears to be established before the SOM processor 40 performs any function. The SOM processor 40 appears to be used to determine what mitigating actions may be taken in response to an attack.

Further, Claim 19 recites "comparing the received predetermined set of data **with expected data values thereof**" (emphasis added). The "expected data values" correspond to data values expected for the target. Appellant respectfully submits that any purported comparison performed by the SOM processor 40 of *Hill* is not with "expected data values" corresponding to the target.

Appellant respectfully submits that for at least this reason, *Hill* does not anticipate Claim 19.

3. 35 U.S.C. § 103 Rejection in view of *Schneier*

a. Claims 18 and 25

Claims 18 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Schneier*.

Appellant respectfully repeats and maintains the arguments presented in Appellant's Appeal Brief regarding Claims 18 and 25, and Appellant respectfully submits that Claims 18 and 25 are patentable over the cited references.

CONCLUSION

Appellant has demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Appellant respectfully requests the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

No fee is believed due with this Reply Brief. If, however, Appellant has overlooked the need for any fee, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

James L. Baudino

James L. Baudino
Registration No. 43,486

Date: January 25, 2008

Correspondence To:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-7917